

INFORME DE AUDITORÍA TI-20-05 (Enm.)

26 de abril de 2020

Autoridad de Edificios Públicos

Oficina de Sistemas de Información

(Unidad 5120 - Auditoría 14282)

Período auditado: 29 de mayo de 2018 al 14 de diciembre de 2018

CONTENIDO

	Página
OBJETIVOS DE AUDITORÍA	2
CONTENIDO DEL INFORME.....	3
ALCANCE Y METODOLOGÍA.....	3
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	4
COMUNICACIÓN CON LA GERENCIA.....	6
CONTROL INTERNO.....	7
OPINIÓN Y HALLAZGOS	8
1 - Deficiencias en la implementación y el funcionamiento de los módulos del Sistema Renova relacionados con la asistencia y las licencias	8
2 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados y de un procedimiento para el manejo de incidentes de seguridad	12
3 - Información incompleta y no actualizada en los anejos del Plan de Contingencia.....	13
RECOMENDACIONES.....	15
APROBACIÓN	17
ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO	18
ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO	19

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

26 de abril de 2020

A la Gobernadora, y a los presidentes del Senado de
Puerto Rico y de la Cámara de Representantes

Incluimos los resultados de la auditoría de tecnología de información que realizamos de la Oficina de Sistemas de Información (OSI) de la Autoridad de Edificios Públicos (Autoridad). Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico, y en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

**OBJETIVOS DE
AUDITORÍA**

Objetivo general

Determinar si las operaciones de la OSI y de los sistemas de información computadorizados de la Autoridad se realizaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

1. Determinar si las operaciones de la OSI; en lo que concierne a los controles internos relacionados con la administración de la seguridad y la continuidad del servicio; se efectuaron, en todos los aspectos significativos, de acuerdo con las normas y reglamentación aplicables; y si dichos controles eran efectivos.
2. Determinar si los módulos Time and Attendance y Human Resources de la aplicación Renova fueron implementados en su totalidad, de acuerdo con los contratos otorgados y los pagos realizados.

**CONTENIDO DEL
INFORME**

Este *Informe* contiene tres hallazgos del resultado del examen que realizamos de los objetivos indicados. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

**ALCANCE Y
METODOLOGÍA**

La auditoría cubrió del 29 de mayo al 14 de diciembre de 2018. En algunos aspectos examinamos transacciones anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de la auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas tales como: entrevistas a funcionarios y empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la entidad auditada o por fuentes externas; pruebas y análisis de procedimientos de control interno, y de otros procesos.

Al realizar esta auditoría utilizamos el *Plan de Contingencia* aprobado el 29 de diciembre de 2010 por el director ejecutivo y las políticas incluidas en la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016 por el director de la Oficina de Gerencia y Presupuesto (OGP). Para las áreas que no estaban consideradas en el *Plan de Contingencias* ni en dichas políticas utilizamos como mejor práctica la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad de Gobierno de Puerto Rico*, según enmendada y las guías establecidas en el *Federal Information System Controls Audit Manual (FISCAM)*¹, emitido por el

¹ El FISCAM utiliza las guías emitidas por el National Institute of Standards and Technology (NIST).

GAO. Esto, porque, aunque a la Autoridad no se le requiere cumplir con dicha *Ley* y guías, entendemos que representan la política pública respecto al control y la contabilidad de los fondos públicos y las mejores prácticas en el campo de la tecnología de información, al examinar los sistemas computadorizados de las entidades gubernamentales.

Consideramos que la evidencia obtenida proporciona una base razonable para nuestra opinión y hallazgos.

Además, relacionado con el segundo objetivo, evaluamos la confiabilidad del informe de transacciones de pagos producido mediante la opción módulo Payments PBA-AP Reports & Consult GUI del módulo de cuentas a pagar del sistema Oracle R12, que contiene, entre otros, el registro de los cheques emitidos a favor de los proveedores de la Autoridad. Como parte de dicha evaluación, entrevistamos a los funcionarios con conocimiento del sistema y de los datos; realizamos pruebas electrónicas para detectar errores evidentes de precisión e integridad en cuanto a los pagos realizados mediante cheques; y revisamos la documentación e información existente sobre los datos y el sistema que los produjo. Determinamos que los datos eran suficientemente confiables para este *Informe*.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Autoridad fue creada mediante la *Ley Núm. 56 del 19 de junio de 1958*, según enmendada. Su propósito principal es satisfacer las necesidades de diseño, construcción, remodelación, mejoras, operación y mantenimiento de las estructuras que necesitan las agencias, corporaciones y entidades del Estado Libre Asociado de Puerto Rico para ofrecer sus servicios. Entre las instalaciones que la Autoridad diseña, construye y conserva, se encuentran: escuelas, hospitales, instalaciones para la policía, cárceles, parques de bomberos y centros de gobierno, entre otras. Además, la Autoridad brinda servicios de arrendamiento de propiedades y nuevos espacios para almacenamiento de servidores (*Data Center*).

Los poderes de la Autoridad son ejercidos por la Junta de Directores (Junta) compuesta por el secretario de Transportación y Obras Públicas, el director de la Autoridad de Asesoría Financiera y Agencia Fiscal de Puerto Rico, el secretario de Educación y otros cuatro miembros nombrados por el gobernador, con el consejo y consentimiento del Senado de Puerto Rico por un término de seis años. El presidente de la Junta es elegido de entre sus miembros. A su vez, dicha Junta nombra al director ejecutivo, quien tiene a su cargo la administración general de la Autoridad y ejerce supervisión sobre todos los funcionarios, empleados y agentes de esta. Los deberes y las responsabilidades de dicha Junta están incluidos en el *Reglamento Interno de la Autoridad de Edificios Públicos (Reglamento Interno)*, revisado el 2 de junio de 2005 por la Junta.

Al 11 de junio de 2018, la estructura organizacional de la Autoridad estaba compuesta por las oficinas de Servicios Legales, Administración, Recursos Humanos y Relaciones Laborales (Oficina de Recursos Humanos), Contraloría, Seguridad Interna, Sistemas de Información, y Comunicaciones Públicas. Para ofrecer los servicios conforme a la *Ley Núm. 56*, cuentan con las áreas de Desarrollo de Proyectos, y Conservación y Mantenimiento. En el Área de Conservación y Mantenimiento se encuentran los directores de las 9 oficinas regionales ubicadas en Aguadilla, Arecibo, Bayamón, Caguas, Carolina, Guayama, Humacao, Mayagüez y Ponce, y los 11 administradores de los centros de gobierno. La Autoridad conserva y mantiene 735 edificios construidos bajo su administración.

La OSI era dirigida por el ejecutivo en sistemas de redes. Además, contaba con dos administradores de sistema de comunicación en red, una analista sistemas de información interina y una secretaria administrativa.

La Autoridad contaba con una red compuesta de 315 computadoras, 42 servidores, 69 *switches*² y 18 *routers*³.

² Dispositivo de comunicación central que conecta dos o más segmentos de red, y permite que ocurran transmisiones simultáneas sin afectar el ancho de banda de la red para una comunicación más eficiente.

³ Dispositivos que distribuyen el tráfico entre redes. La decisión sobre dónde enviar los datos se realiza a base de la información de nivel de red y las tablas de direccionamiento.

Los recursos para financiar las actividades operacionales de la Autoridad provienen de ingresos propios recibidos del arrendamiento de sus instalaciones físicas, asignaciones especiales y otros ingresos. Los gastos operacionales de la OSI son sufragados por el presupuesto operacional de la Autoridad que, para los años fiscales del 2016-17 al 2018-2019, ascendió a \$107,432,028, \$91,144,940, y \$104,660,327, respectivamente.

Los **anejos 1 y 2** contienen una relación de los miembros de la Junta y los funcionarios principales de la Autoridad que actuaron durante el período auditado.

La Autoridad cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.aep.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones determinadas durante la auditoría fueron remitidas al Sr. Josean Nazario Torres⁴, entonces director ejecutivo, mediante cartas del 10 de enero y el 25 de febrero de 2019.

El entonces director ejecutivo contestó la carta del 1 de febrero; y la del 25 de febrero la contestó la Sra. Yanis Morales Gracia, subdirectora ejecutiva, en su representación. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

El 5 de febrero de 2020 remitimos el borrador de este *Informe* a la Sra. Melitza López Pimentel, directora ejecutiva; el borrador de los hallazgos de este *Informe* al señor Nazario Torres y el borrador del **Hallazgo 1** al Dr. Amílcar González Ortiz; ex directores ejecutivos. Además, mediante correo electrónico del 4 de marzo, remitimos el borrador del **Hallazgo 1** al Ing. José L. Dávila Estrada y al Ing. Ángel L. González Carrasquillo, ex directores ejecutivos.

⁴ Según noticia del periódico El Vocero este renunció a su cargo el 16 de julio de 2019.

El 5 de marzo de 2020 la Sra. Milka M. Sierra Castro, directora de Calidad y Eficiencia, en representación de la directora ejecutiva, nos contestó que luego de evaluar la información y el borrador de este *Informe* determinaron no emitir comentarios al respecto.

El ex director ejecutivo Nazario Torres contestó mediante correo electrónico del 21 de febrero de 2020 e indicó lo siguiente:

Los hechos que motivan el hallazgo son situaciones que la Autoridad enfrenta desde antes del 2018 y surgen bajo determinaciones y actuaciones de pasadas administraciones de la AEP. Tomé posesión como Director Ejecutivo el 20 de julio de 2018. Una vez tome posesión como Director Ejecutivo de la AEP iniciamos gestiones encaminadas a atender las deficiencias señaladas en el hallazgo. Incluyendo evalué la conveniencia de finalizar los contratos objeto del señalamiento y considerar otras opciones que pudieran ayudar en tomar medidas correctivas en el asunto. Sin embargo, nuestra gestión administrativa cesó antes de que pudiéramos diseñar e implementar planes estratégicos y acciones afirmativas para corregir las situaciones señaladas. [sic]
[Hallazgo del 1 al 3]

El doctor González Ortiz contestó mediante correo electrónico del 1 de marzo de 2020 e indicó, entre otras, cosas que el contrato y sus tres enmiendas fueron otorgados por el director ejecutivo que lo precedió. Además, él comenzó como director ejecutivo el 9 de febrero de 2017 y el ejecutivo en sistemas de redes solicitó, como perito en el área, que se le extendiera el contrato a la compañía contratada para que terminara de implementar el sistema.

Los ingenieros Dávila Estrada y González Carrasquillo no contestaron.

CONTROL INTERNO

La gerencia de la Autoridad es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera
- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para los objetivos de esta auditoría. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno de la Autoridad.

En los **hallazgos 2 y 3** de este *Informe* se comentan deficiencias de control interno significativas, dentro del contexto de los objetivos de nuestra auditoría, identificados a base del trabajo realizado.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con los objetivos de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la OSI y la Autoridad objeto de este *Informe* se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que los controles establecidos eran efectivos. Esto, excepto por los **hallazgos del 1 al 3** que se comentan a continuación.

Hallazgo 1 - Deficiencias en la implementación y el funcionamiento de los módulos del Sistema Renova relacionados con la asistencia y las licencias de los empleados

Situaciones

- a. Las entidades deben adquirir, desarrollar e implementar aplicaciones, programas, equipos y productos tecnológicos con soluciones de alta calidad y efectividad, y asegurarse de que el gasto en esta inversión se realice en un marco de utilidad y austeridad. La tecnología adquirida debe promover una infraestructura capaz de aumentar su funcionalidad e interactuar con otros sistemas, para mejorar su rendimiento y las capacidades operacionales necesarias para ofrecer

un servicio gubernamental de alta calidad. Además, para garantizar la utilidad de los sistemas, se deben realizar pruebas para validar que, en cada etapa de su ciclo de vida, este cumple con los requerimientos funcionales y de seguridad requeridos.

Del 30 de abril de 2015 al 18 de julio de 2018, la AEP otorgó tres contratos y tres enmiendas por \$129,813, a una compañía para la implementación de un sistema (Sistema Renova) que incluyera, entre otros, los módulos de Time and Attendance y el de Human Resources.

El módulo Time and Attendance permitiría realizar los procedimientos para el registro de la asistencia, la configuración del horario de trabajo de los empleados, necesario para el cálculo automático de la nómina y los balances de licencias. El módulo Human Resources permitiría realizar los procedimientos relacionados con la administración de los recursos humanos, tales como, certificaciones e informes de empleados activos. Al 1 de octubre de 2018, la AEP había pagado \$102,776 de dichos contratos.

El examen sobre la implementación y el funcionamiento de los módulos Time and Attendance y Human Resources del Sistema Renova reveló lo siguiente:

- 1) Relacionado con el módulo Time and Attendance existían las siguientes situaciones:
 - a) No se calculaban correctamente los balances de las licencias.
 - b) Se revertían los cambios de horario registrados para un empleado.
 - c) No se actualizaba, en los relojes ponchadores, los cambios relacionados con la asignación del personal autorizado a registrar su asistencia.
 - d) En ocasiones, los ponches para registrar la asistencia del personal no se registraban en el módulo. Esto, a pesar de que el reloj ponchador indicaba que aceptaba el registro.

- e) Se registraban descuentos de horas, minutos y tardanzas sin razón alguna.

Mediante entrevistas realizadas el 29 y 31 de enero de 2019 a una oficinista V y la asistente administrativa de la Oficina de Recursos Humanos, estas nos indicaron que las situaciones indicadas en los **apartados del b) al e)** fueron discutidas con la compañía en reuniones realizadas el 17 de junio (previo al otorgamiento del tercer contrato) y el 17 de octubre de 2018.

- 2) Al 29 de enero de 2019, según la coordinadora de recursos humanos y relaciones laborales, no se habían corregido las siguientes situaciones que fueron identificadas en el módulo Human Resources:
 - a) Ocurrían interrupciones continuas en la conexión al módulo, que fluctuaban entre horas y semanas sin servicio. Según los correos electrónicos suministrados el 21 de febrero de 2019 por la analista de sistemas de información interina, la coordinadora de recursos humanos informó, entre el 28 de noviembre de 2018 y el 29 de enero de 2019, sobre las últimas tres interrupciones que habían ocurrido.
 - b) La certificación de empleo que producía el módulo para ser emitida a la Asociación de Empleados del Estado Libre Asociado de Puerto Rico no incluía información en todos los campos requeridos. Entre estos, la fecha en que el empleado comenzó a cotizar los ahorros, fecha del último descuento de ahorros, el sueldo neto del empleado y la fecha de la certificación.
 - c) La pantalla Reports\Job Incumbency del puesto de director ejecutivo presentaba períodos de incumbencia incorrectos. Estos períodos se creaban cuando era necesario reactivar los registros de exfuncionarios en el módulo de Human Resources, para que se pudieran procesar los pagos de liquidación de licencia mediante el módulo de Payroll.

Crterios

La situación comentada es contraria a lo establecido en el Artículo 2(g) de la *Ley Núm. 230* y en la sección Política de la *ATI-013* de la *Carta Circular 140-16*.

Efectos

Las situaciones comentadas no le permiten a la Autoridad obtener todos los beneficios esperados de los \$102,776 invertidos en los módulos del sistema Renova y que incluían el proceso automatizado para el registro de la asistencia, la acumulación y utilización de las licencias de los empleados, el control de los balances de estas y el manejo de asuntos administrativos como la producción de informes y certificaciones. Además, según indicado por la asistente administrativa de la Oficina de Recursos Humanos, ocasionaba atrasos en las operaciones de esta Oficina que estaban relacionadas con el procesamiento de las asistencias y la nómina del personal. También la oficinista V de la Oficina de Recursos Humanos nos indicó que tiene que mantener manualmente los balances de las licencias de los empleados del Centro Gubernamental de Carolina, del Centro Judicial Guayama, y de las regiones de Caguas, Carolina, Guayama y Mayagüez. Esto, a su vez, puede propiciar la comisión de errores o irregularidades en el cálculo de las licencias y el registro de la asistencia, sin que se puedan detectar a tiempo para corregirlos y fijar responsabilidades.

Causas

Las situaciones comentadas en el **apartado a.1)** se debían a que durante la implementación de los módulos del sistema Renova hubo cambios continuos del personal de la Autoridad asignado a supervisar dicho proyecto. Esto afectó la continuidad de los procesos iniciados y la supervisión adecuada del proyecto. Además, según la coordinadora de recursos humanos, las situaciones comentadas en el **apartado a.2)** se

debieron a que la compañía realizó las pruebas en ambiente producción y cuando realizaba cambios, en ocasiones se afectaban otras funcionalidades del módulo que trabajaban correctamente.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados y de un procedimiento para el manejo de incidentes de seguridad

Situaciones

- a. Un análisis de riesgo es un proceso mediante el cual se identifican los activos de los sistemas de información, sus vulnerabilidades y las amenazas a las que están expuestos. Además, se establecen las medidas de seguridad y controles adecuados para evitar o disminuir los riesgos y proteger los activos. Toda entidad gubernamental debe realizar un análisis de riesgos, al menos, cada 24 meses o luego de un cambio significativo en la infraestructura operacional.

Al 24 de septiembre de 2018, en la Autoridad no se había preparado un informe de análisis de riesgos de los sistemas de información computadorizados.

- b. Las agencias deben desarrollar procedimientos para identificar, informar y responder a incidentes de seguridad, incluidos aquellos que causen interrupción en la prestación de sus servicios. Estos procedimientos deben identificar el personal asignado para responder a los incidentes de seguridad e incluir los límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta.

Al 24 de septiembre de 2018, la Autoridad no contaba con un procedimiento o plan para el manejo de incidentes de seguridad relacionados con sus sistemas de información computadorizados.

Criterios

Lo comentado es contrario a lo establecido en las secciones A. y F. de la *Política ATI-003, Seguridad de los Sistemas de Información*, y en las secciones C. y E. de la *Política ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*.

Efectos

La situación comentada en el **apartado a.** impide a la Autoridad estimar el impacto que los elementos de riesgos tendrían en las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

Lo comentado en el **apartado b.** puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

Causas

La situación comentada en el **apartado a.** se atribuye a que, según el ejecutivo en sistemas de redes, la Autoridad no contaba con recursos internos adiestrados para preparar el análisis de riesgos conforme a las mejores prácticas de los sistemas de información computadorizados.

La situación comentada en el **apartado b.** se debía a que, según el administrador de sistema de comunicación en red, no había recibido una directriz de alguno de sus supervisores⁵ para la preparación del procedimiento o plan para el manejo de incidentes de seguridad.

Véanse las recomendaciones 1 y de la 3 a la 5.a.

Hallazgo 3 - Información incompleta y no actualizada en los anejos del Plan de Contingencia**Situación**

- a. En el *Plan Operacional de Emergencia* de la Autoridad se establece que la OSI es responsable de coordinar con las demás oficinas y regiones la protección del equipo de la Autoridad. Una vez concluida la emergencia, debe incorporarse el personal necesario para mantener el sistema funcionando y trabajar con los programas necesarios. Como parte de dicha responsabilidad, el 29 de diciembre de 2010 el entonces director ejecutivo de la Autoridad aprobó el *Plan de Contingencia (Plan)* para asignar funciones específicas y fijar

⁵ Durante el período auditado, la OSI fue dirigida por cuatro funcionarios que ocuparon el puesto de ejecutivo en sistemas de redes.

responsabilidades al personal de la OSI, tales como mantener actualizada la información incluida en el *Plan*, la preparación del centro de cómputos alternativo, y establecer medidas para evitar, detectar y prevenir la ocurrencia de incidentes que puedan provocar la pérdida de equipo y datos.

El examen realizado el 12 de octubre de 2018 reveló las siguientes deficiencias en los anejos del *Plan*:

- 1) El Anejo V-1, Lista de Empleados de la Oficina de Sistemas de Información, contenía el nombre de cinco exempleados. Además, no incluía la información de contacto de cuatro empleados de la OSI, ni el nombre y la información de contacto de una asistente administrativa que laboraba en dicha Oficina.
- 2) El Anejo V-4, Lista de Prioridades Establecidas con Relación a los Sistemas, incluía el sistema de asistencia Kronos, que no era utilizado por la Autoridad; y no incluía el sistema Renova.
- 3) El Anejo V-5, Lista de Compañías de Servicios de Mantenimiento de Equipos, no incluía cuatro proveedores que, a la fecha de nuestro examen, ofrecían servicios de mantenimiento a la OSI, e incluía un proveedor que no ofrecía servicios.
- 4) El Anejo V-9, Lista de la Documentación del Sistema a Utilizar, el cual debía contener los manuales de los sistemas operativos en producción, incluía el sistema Unix, que no era utilizado en la Autoridad.
- 5) El Anejo V-10, Lista de Equipos de Computadoras de la OSI, no identificaba los equipos asignados a los cuatro empleados de la OSI e incluía el nombre de cinco exempleados.
- 6) En el Anejo V-11, Lista de Equipo de Computadora del Centro de Cómputos, incluía 11 servidores con descripción que no coincidía con la lista de servidores de la Autoridad, que nos fue suministrada el 12 de julio de 2018 por el administrador de sistemas de comunicación en red.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la Sección 5.10 E. del *Plan de Contingencia* aprobado el 29 de diciembre de 2010.

Efectos

La situación comentada puede propiciar la improvisación, y que, en casos de emergencia, se tomen medidas inapropiadas. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, e interrupciones prolongadas de los servicios a los usuarios de la Autoridad. Además, lo comentado no le permite a la Autoridad ejercer un control adecuado sobre las operaciones de la OSI, ni les permite a los empleados y funcionarios de la Autoridad contar con procedimientos que estén cónsonos con los cambios tecnológicos, administrativos, operacionales y organizacionales.

Causas

El 15 de octubre de 2018, el entonces director ejecutivo nos informó que la situación comentada se debía a que el exejecutivo en sistemas de redes no completó la actualización del *Plan* antes de culminar sus labores el 24 de agosto de 2018. Además, el entonces director ejecutivo y el ejecutivo en sistemas de redes informaron que la Autoridad no contaba con recursos internos para actualizar el *Plan* conforme a las mejores prácticas de los sistemas de información computadorizados.

Véanse las recomendaciones 1, 3 y 5.b.

RECOMENDACIONES**A la Junta de Directores de la Autoridad**

1. Ver que la directora ejecutiva de la Autoridad cumpla con las **recomendaciones de la 2 a la 5** de este *Informe*. [**Hallazgos del 1 al 3**]

A la directora ejecutiva de la Autoridad

2. Asegurarse de que se tomen las medidas necesarias para que se corrijan las deficiencias comentadas en el **Hallazgo 1**, que afectan la funcionalidad de los módulos Time and Attendance y Human Resources del sistema Renova.
3. Ver que se ofrezca al personal de la OSI los adiestramientos necesarios para capacitarlos en la preparación de un análisis de riesgo, el plan para el manejo de incidentes de seguridad y el plan de contingencia. **[Hallazgos 2 y 3]**
4. Asegurarse de que se realice y se documente un análisis de riesgos que considere los sistemas de información computadorizados de la Autoridad, según se establece en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. Una vez aprobado, ver que se revise cada vez que surja un cambio significativo dentro de la infraestructura operacional y tecnológica de la Autoridad. Esto, para asegurarse de que se mantenga actualizado. **[Hallazgo 2-a.]**
5. Ejercer una supervisión efectiva sobre el ejecutivo en sistema de redes para asegurarse de que:
 - a. Prepare y remita para su aprobación un procedimiento relacionado con el manejo de incidentes. Como parte de dicho procedimiento, se debe requerir que se documenten todos los incidentes y se indique cómo se resolvieron de manera que, cuando estos se repitan, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información y la continuidad de las operaciones. **[Hallazgo 2-b.]**
 - b. Revise y remita, para su aprobación, el *Plan* y se asegure de que el mismo incluya la información actualizada de los aspectos comentados en el **Hallazgo 3**.

APROBACIÓN

A los funcionarios y a los empleados de la Autoridad, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por:

A handwritten signature in blue ink, appearing to read "Jamin M. Calderin".

ANEJO 1

**AUTORIDAD DE EDIFICIOS PÚBLICOS
OFICINA DE SISTEMAS DE INFORMACIÓN
MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Ing. José Izquierdo Encarnación	Presidente	29 may. 18	14 dic. 18
Lcdo. José A. Flores Díaz	Secretario	1 nov. 14	14 dic. 18
Sra. Aileen I. Mojica de Jesús	Secretaria Interina	29 may. 18	31 oct. 18

ANEJO 2

AUTORIDAD DE EDIFICIOS PÚBLICOS
OFICINA DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Josean Nazario Torres	Director Ejecutivo	20 jul. 18	14 dic. 18
Dr. Amílcar González Ortiz	"	29 may. 18	19 jul. 18
Sra. Yanis Morales Gracia	Subdirectora Ejecutiva	9 ago. 18	14 dic. 18
Sr. Josean Nazario Torres	Subdirector Ejecutivo	29 may. 18	19 jul. 18
Sra. Yanis Morales Gracia	Ejecutivo en Sistemas de Redes	20 oct. 18	14 dic. 18
Sr. Anthony Otero Quintana	Ejecutivo Interino en Sistemas de Redes	13 sep. 18	19 oct. 18
Sr. Edwin Jiménez Barreto	"	27 ago. 18	12 sep. 18
Sr. Luitpoldo Marrero Ramírez	Ejecutivo en Sistemas de Redes	29 may. 18	24 ago. 18

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-18-19* del 27 de abril de 2018, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensiones 2801 o 2805, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos y el tipo de opinión del informe.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el administrador de documentos al (787) 754-3030, extensión 3400.

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069